Inter-Agency Misconduct Disclosure Scheme

Frequently Asked Questions

(work in progress – please send questions to add or amend to schr@ifrc.org)

Concerning GDPR compliance:

- *What is the lawful basis for processing under the Scheme?*

  Processing (sharing) of candidates' personal data under the Scheme is considered to be necessary for the purposes of the legitimate interests pursued by the Requesting Organisation (i.e. the latter's legitimate interests as data controller and those of a "third party" from the perspective of the Responding Organisation, pursuant to Article 6 § 1 let. f GDPR). The conception under the Scheme is that the legitimate interests pursued by the Requesting Organisation are *not* overridden by the interests or fundamental rights and freedoms of the candidates (data subjects).

  The processing (disclosure) of personal data by the Responding Organisation can also be considered to be necessary for the purposes of its legitimate interests, i.e. the interest of disclosing relevant information about a current or former employee to a prospective employer.

  It can also be argued that processing under the Scheme is necessary for the performance of a task carried out in the public interest. Indeed, Participating Organisations are all pursuing missions of public interest, which justify the very high requirements that they set in terms of integrity for their employees, which in turn render necessary the sharing of personal data contemplated by the Scheme.

- *What are the main GDPR compliance requirements that apply to the Scheme?*

  All principles relating to the processing of personal data under the GDPR apply in the context of the Scheme, namely:

  - Transparency: the purpose and means of processing are made accessible to data subjects.
  - Purpose limitation: personal data is processed under the Scheme for the specified and explicit purpose of recruitment.
  - Data minimisation: the data shared is limited to what is necessary in relation to the purposes for which it is processed.
  - Accuracy: every step is taken to ensure that the data is accurate.
  - Storage limitation: the Scheme prescribes time limitations around the retention and sharing of data.
  - Integrity and confidentiality: the Scheme enjoins Participating Organisations to take measures to protect data from unauthorised or unlawful processing and against accidental loss, destruction or damage.
  - Controller accountability: each Participating Organisation subject to the GDPR is responsible for demonstrating compliance with its requirements.

Each Participating Organisation should adopt an implementing policy to the Scheme, as prescribed at Article 5.7 of the Scheme, which may provide further details on the way these principles and other GDPR requirements are met concretely.

- *What are the main GDPR non-compliance risks of the Scheme?*

One risk is that the sharing of personal data may not be considered as necessary in each and every case, on the basis that the level and nature of information to be gathered with respect to a candidate in a recruitment process should vary and depend on the particular position for which the candidate is applying.

Another risk could be around transfers of personal data outside the EU for purposes of the Scheme. While the Scheme is silent on this aspect, it seems clear that the corresponding requirements of the GDPR (Articles 44 ff.) apply.

The group of Participating Organisations that has developed the Scheme had undertaken to carry out a data protection impact assessment (DPIA), which is both a compliance measure under the GDPR where risks around the processing of personal data are identified, and a way to reduce such risks, thereby bringing the processing operations in line with applicable requirements, in particular the principle of proportionality.

- *What are the HR procedures which organisation can consider, to reduce non- compliance risks?*

In general, Participating Organisations should adopt implementing procedures which :

- favour transparency around processing, notably through the use of tailored privacy notices and other communications to employees and candidates that set out as clearly as possible the way personal data is processed in the context of the Scheme
- guarantee data subjects' rights throughout the process, including the right of access (see Article 5.3.3 of the Scheme);
- ensure that all actions taken under the Scheme are properly documented;
- contain provisions or references to internal policies that provide for appropriate technical and organisational security measures that cover all HR systems and functions, including 'need-to-know' access limitations, encryption and regular training / guidance and adequately address data breaches (whether electronic or physical) (see Article 5.3.3 of the Scheme); and
- are well embedded into a general policy around vetting and referencing in the recruitment context that sets out the principles and processes according to which these activities are conducted within the organisation.

- *Do these measures need to apply to all cases, or only to Candidates who have been found to have committed Misconduct (as defined by the Scheme)?*

These measures apply to the processing of personal data, which means that they apply whenever a Participating Organisation is dealing with personal data under the Scheme in one

way or another. The way the measures apply also depends on the type of processing and the nature of the data processed. For example, Participating Organisations should ensure transparency on the Scheme and the way they apply it to all their employees and candidates. On the other hand, processing requirements around information related to a Misconduct (both on the Requesting Organisation's and the Responding Organisation's side) will apply only to data subjects (employees/candidates) who have been found to have committed Miscconduct.